Amendments to the Claims

1. (original) A system comprising:

a blade device; and

chassis management logic, the chassis management logic to determine whether one or more capabilities associated with the blade device match a capability policy.

2. (original) The system of claim 1, further comprising:

a data communication pathway coupled to the blade device and to the chassis management logic.

3. (original) The system of claim 1, wherein:

the chassis management logic is further to isolate the blade device from a computing domain responsive to determining that the blade device capabilities do not match the capability policy.

4. (original) The system of claim 1, further comprising:

a plurality of blade devices;

wherein each of the plurality of blade devices is coupled to the data communication pathway; and

wherein the chassis management logic is further to determine, for at least one of the plurality of blade devices, whether blade capabilities associated with the at least one blade device match the capability policy.

5. (original) The system of claim 4, wherein:

the chassis management logic is further to isolate from the computing domain any of the plurality of blade devices whose associated capabilities do not match the capability policy.

6. (original) The system of claim 1, wherein:

the chassis management logic is further to determine whether the blade device is trusted.

7. (original) The system of claim 1, further comprising:

a baseboard memory controller, wherein the baseboard memory controller is to control communication between the blade device and the chassis management logic.

8. (original) The system of claim 1, wherein:

the blade device includes logic to perform boot processing.

9. (original) The system of claim 8, wherein:

the chassis management logic is further to generate a failure indicator value responsive to determining that the blade device capabilities do not match the capability policy; and

the blade device is to, responsive to the failure indicator value, terminate the boot processing.

10. (original) The system of claim 1, further comprising:

a chassis to receive the blade device.

11. (original) A method comprising:

determining if one or more capabilities associated with a blade device match a capability policy; and

if the blade device capabilities do not match the capability policy, isolating the blade device from a computing domain.

12. (original) The method of claim 11, further comprising:

challenging the blade device to provide a response; and

if the blade device does not provide the response, isolating the blade device from the computing domain.

13. (original) The method of claim 11, wherein determining further comprises:

accessing a capability record associated with the blade.

14. (original) The method of claim 11, further comprising:

maintaining in a central repository a plurality of capability records, each capability record being associated with one of a plurality of blade devices.

15. (original) The method of claim 12, wherein challenging further comprises:

encrypting a challenge value using a public key value; and

providing the encrypted challenge value to the blade device.

16. (original) The method of claim 11, further comprising:

maintaining in a central repository a plurality of public key values, each of the public key values corresponding to one of a plurality of blade devices.

17. (original) An article comprising:

a machine-readable storage medium having a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

registering one or more capabilities with a central repository;

determining if one or more capabilities associated with a blade device match a capability policy; and

if the blade device capabilities do not match the capability policy, isolating the blade device from a computing domain.

18. (original) The article of claim 17, further comprising:

a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

challenging the blade device to provide a response; and

if the blade device does not provide the response, isolating the blade device from the computing domain.

19. (original) The article of claim 17, wherein:

the instructions that cause the machine to determine if one or more capabilities associated with a blade device match a capability policy further comprise instructions that cause the machine to access a capability record associated with the blade.

20. (original) The article of claim 17, further comprising:

a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

maintaining in a central repository a plurality of capability records, each capability record being associated with one of a plurality of blade devices.

21. (original) The article of claim 18, wherein:

the instructions that cause the machine to challenge further comprise instructions that cause the machine to :

encrypt a challenge value using a public key value; and

provide the encrypted challenge value to the blade device.

22. (original) The article of claim 17, further comprising:

a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

maintaining in a central repository a plurality of public key values, each of the public key values corresponding to one of a plurality of blade devices.

23. (original) A method comprising:

registering one or more capabilities with a central repository;

determining if a capability authorization has been received within a pre-defined timeout interval;

if the capability authorization has been received within the timeout interval, performing boot processing; and

if the capability authorization has not been received within the timeout interval, declining to perform the boot processing.

24. (original) The method of claim 23, further comprising:

providing a response to a challenge;

proceeding, if the response is correct, with boot processing; and

if the response is not correct, isolating from a computing domain.

25. (original) The method of claim 24, wherein:

providing a response further comprises decrypting a challenge value using a private key.

26. (original) The method of claim 23, wherein:

declining to perform the boot processing further comprise performing stand-alone boot processing.

27. (original) The method of claim 23, wherein:

declining to perform the boot processing further comprises powering down.

28. (original) An article comprising:

a machine-readable storage medium having a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

registering one or more capabilities with a central repository;

determining if a capability authorization has been received within a pre-defined timeout interval;

if the capability authorization has been received within the timeout interval, performing boot processing; and

if the capability authorization has not been received within the timeout interval, declining to perform the boot processing.

29. (original) The article of claim 23, further comprising:

a plurality of machine accessible instructions, which if executed by a machine, cause the machine to perform operations comprising:

providing a response to a challenge;

proceeding, if the response is correct, with boot processing; and

if the response is not correct, isolating from a computing domain.

30. (original) The article of claim 24, wherein:

instructions that cause the machine to provide a response further comprise instructions that cause the machine to decrypt a challenge value using a private key.

31. (original) The article of claim 23, wherein:

instructions that cause the computer to decline to perform the boot processing further comprise instructions that cause the machine to perform stand-alone boot processing.

32. (original) The article of claim 23, wherein:

instructions that cause the computer to decline to perform the boot processing further comprise instructions that cause the machine to power down.

33. (newly added) The system as recited in claim 1, wherein the chassis management logic further comprises authentication logic to determine whether the blade device is to be authenticated before determining whether one or more capabilities associated with the blade device match the capability policy.

34. (newly added) The system as recited in claim 1, wherein the chassis management logic is to register the one or more capabilities associated with the blade device with a central repository, and determine whether the one or more registered capabilities associated with the blade device match the capability policy, resulting in a capability authorization;

if the capability authorization has been received within a predetermined timeout interval, the chassis management logic to allow boot processing of the blade device; and

if the capability authorization has not been received within the predetermined timeout interval, then the chassis management logic to disallow the boot processing of the blade device.